Alles Betrug - Internet Live!

Das große Geld mit Internetdialer und Sie werden zur Kasse gebeten.

Vor Jahren klingelten merkwürdige Gestalten an der Tür um wenigstens ein Zeitungsabo zu verkaufen und die Leute auf diese Art und Weise abzuzocken.
Nicht das sich die Zeiten der recht seltsamen Handelsvertreter groß geändert hat, aber das Internet kam hinzu und somit auch die Chancen die Leute dort abzuzocken.

In einigen Berichten habe ich davon geschrieben, wie man Sie durch 0190-Dialer im Internet knallhart des hart verdienten Geldes beraubt.
Die Abzocke weitet sich aber derzeit soweit aus, dass in allen Kommunikationsmitteln ein Weg gesucht wird, ahnungslose Menschen zu betrügen.
Besonders stark ist in der letzten Zeit wieder aufgefallen, dass Internetbenutzer mit falschen Domains in die Irre geführt werden.
Die echten Domains haben in 99% der Fälle nichts mit einem solchen Betrug zu tun, aber es ist täuschend echt gestaltet.

So ereignet sich gleich Anfang Januar ein Fall, der recht interessant war und auf den ich hier kurz eingehen möchte.
Hier geht es um die **FALSCHE** Domain www.edonkey.com die sich von der echten Domain nur um die Zahl 2000 unterscheidet.
Die echte Domain der Tauschbörse heisst also www.edonkey2000.com.
Auf der falschen Domain findet man dann diverse Dialer, die von einem deutschen Betreiber aus teure 0190 Nummer durch das Internet anwählen und somit Ihren Geldbeutel erleichtern.
Hinter einigen Seiten stecken zumeist harmlos erscheinende Programme wie "MP3_Plugin.exe" die sich aber dann als Trojanische Pferde enttarnen.
Diese übermitteln Userdaten, Surfverhalten und ermöglichen den Zugriff auf den Computer, der dann mit einem Dialer versehen wird.
Weitere Informationen dazu:

http://www.brain-pro.de/Seiten/advisory/advisor1.htm

Die Betreiber sind oftmals unscheinbar und kommen aus Aachen oder Dresden oder aus irgendeiner Kleinstadt wo vielleicht auch Sie wohnen und abgezockt werden.

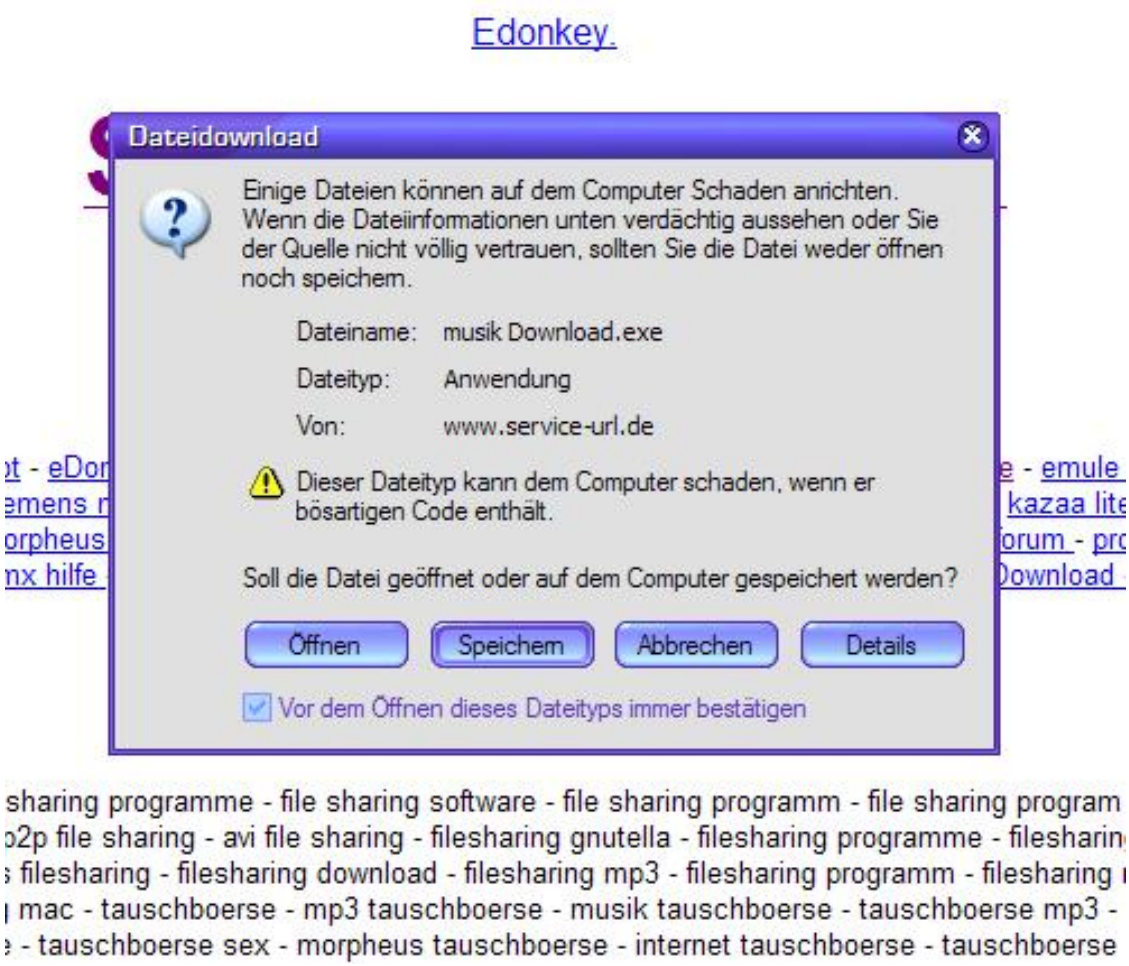
Wärend Sie nun durch einen Dialer missbraucht im Internet surfen, merken Sie nicht mal das Ihr Handy klingelt.
Sie schauen verwundert auf das Telefon und stellen nur noch einen "Anruf in Abwesenheit" fest, der Sie aber sicherlich interessieren wird.
Beim nachschauen stellen Sie nichts besonderes fest, drücken auf die "wähl-Taste" und rufen eine 0137-Nummer an.
Diese Nummer ist bis dahin auch noch unscheinbar, bis eine Umleitung aktiv wird, und zu einer 0190-Nummer weiter schaltet.
Nun kann es durchaus sein, dass dadurch Kosten von mindestens 1 Minute 50 Cent bis 1,20 Euro abgerechnet und fällig werden.
Bis dahin sind Sie zunächst einmal machtlos, denn es wurde sogar schon davon berichtet, dass bei einigen solcher dubiosen Dienste gleich eine ganze Stunde abgerechnet und verbucht wird. Vom Handy!

Damit noch nicht genug.
Es gibt derzeit so viele verschiedene Möglichkeiten Sie um das hart verdiente Geld zu bringen, dass ich schon fast ein Buch damit füllen könnte.
Interessant finde ich nach wie vor eine Möglichkeit, die sich ein junger Mann zu nutze gemacht hat, um das Internet mit Dialer vollzumüllen!

Der Fall Emule.biz!

Eine Domain, die vielen möglicherweise ein Begriff sein dürfte da es hier auch um Filesharing geht.
Normal kann man davon ausgehen, dass kein böswilliger Hintergrund zu sehen ist, jedoch ist es hier in diesem Fall anders.
Man registriert viele Internetseiten bei einem Hoster, packt hinter jedem Link seine eigene Homepage und "gestaltet" das ganze mit vielen 0190-Dialern.

Da wird auf der einen Seite eine Hilfe und der Download von Emule angeboten und ehe man sich versieht, tut sich etwas völlig anderes auf:
http://install.stardialer.de/?account=XXXXXXXXXXX.
Es öffnet sich beim draufklicken eine Seite, die dann gleich die Zugangssoftware installieren will.



Das es sich hierbei **nicht** um eine Zugangssoftware handelt, sollte hier jedem bewusst sein.
Weiterhin kann man eine Emule Serverliste und ein angebliches Forum besuchen, dass dann aber auf die gleiche Installationsseite geht wie der oben angeschriebene Dialer.
Unter den Filesharing Listen befinden sich dann weitere Links auf identische Seiten:

edonkey-morpheus-forum.de, file-sharing-forum.de, filesharing-forum.de, morpheus-forum.de, edonkey-2000.de, edonkey-bot.de, edonkey-edonkey2000.de, edonkey-hilfe.de, kazaa-hilfe.de, winmx-hilfe.de.

Nun haben Sie den Sprung geschafft und sind der Meinung, wenn Sie auf www.1md.de gehen, dann kommt man zum Urheber der Seite wo man dann Kaza downloaden kann. Aber hier sieht man gleich wieder eine Installation: http://install.stardialer.de/?account=XXXXXXXXXXX.

Beworben wird das ganze geschickt hiermit:
KaZaA Lite Download - KaZaA Lite Hilfe - KaZaA Lite Beschreibung - deutsche FAQ zu KaZaA Lite - KaZaA Lite Forum.

Ich surfe nun schon seit ca. 20 Minuten mit meiner Zugangssoftware und habe in dieser Zeit durch das Wirrwarr an Seiten 10 PopUp Fenster schliessend müssen.
Endlich scheint es dann aber geschafft zu sein.
Ich habe nun verstanden, dass sich **hinter den meisten Links ein Dialer befindet** und sehe einen großen Link:
" SOFORT ZUM FORUM". Das muss es sein.

Ich klicke drauf und schwups passiert es wieder, ein Download startet.
Leider funktioniert der direkte Link auf das Hilfe-Filesharing-Forum auch nicht korrekt:
http://install.stardialer.de/?account=XXXXXXXXXX;

wieder ein Dialer. Eine wahre Rekordmarke scheint sich anzubahnen.
Aha, nun aber doch auf einer von den vielen Seiten des Betreibers ein seltsamer Hinweis:
"*Die Benutzung unserer Angebote Hilfen und Downloads kostet vom nationalen Festnetz aus den angegeben Preis von 1,86 €Min.
Wichtiger Hinweis: Unsere Download Angebote enthalten NICHT die Programme selbst sondern Hilfe und Informationen zu diesen."

Hinter einigen Links auf einer der vielen Seiten, stecken dann abermals einige 0190-Dialer. Zum Beispiel hinter einem vermutetem SMS Archiv startet der nächste Download.

Da ich mich nun weiter für diese Seiten interessiere, verbinde ich mich mit einem der Provider dieser Seiten und rufe direkt bei der Firma HOST EUROPE GmbH in Köln an.
Zunächst ist dem Unternehmen mein Anruf zweimal so wichtig, dass ich laut der freundlichen Damenstimme dran bleiben soll bis der Anruf dann letzlich doch abgebrochen wird.
Weitere Kontaktaufnahmen blieben erfolglos.

Ein weiterer Provider ist Puretec.
Dort kann man auch versuchen telefonisch Kontakt aufzunehmen, was dann über eine 0190 Nummer oder eine 0180 Nummer ermöglicht wird.
Von einer Servicemitarbeiterin dort erhielt ich den Hinweis, dass aufgrund der AGBs dort ein Hosting betrieben wird und man sich nicht dafür zuständig erklärt.
Inhalte werden also nicht geprüft, wieso auch.

Ein weiterer Hoster scheint webcockpit.de zu sein, der über eine Internetadresse nicht eindeutig zu ermitteln ist.
Laut der offiziellen Denic Abfrage gehört diese Domain KPNQuest in Karlsruhe, einem weiteren großen Provider.

MoMolly, ein Mitglied der Kryptocrew berechnete den Gewinn der Person, die auf all diesen Seiten einen Dialer installiert hat.
Dabei wurde angenommen, dass je Dialer 1,89 Euro je ag einen Dialer installieren und im guten Gla#8364; a.Tag, (30Tage) = 850.500 €i.Monat, dass macht im Jahr die stolze Summe von 10.206.000,- €
Dies sollte nur mal ein ausführliches Beispiel sein.

Der Betreiber hinter den Domains hat in einem Forum öffentlich nach der Verlinkung von ca. 1500 Domains gefragt um sich untereinander ein großes Portal mit Dialern zu schaffen.
Hier ein **Auszug** aus dem posting:

"Mal eine Frage an die experten zum Thema "Wie verlinke ich richtig"
(Das Thema wurde hier im Forun meiner Meinung nach zuwenig behandelt)
Also mein Problem ist:
Ich habe ca. 1500 Domains mit folgenden endungen registriert .be .ag .de .com .info .biz .net .org .at .li .ch .co.uk.org.uk .me.uk .tv .cc alles bunt gemischt und in verschiedener anzahl einige Domain Namen mit jeder endung andere nur mit denen die frei wahren.
Es sind 20 Domains (jede Domain ist mit jeder verlinkt) mit hohen PR (5-6) und 5000 Unterseiten zu den 20 Domains mit PR ab 4 verfügbar.
Wie verlinke ich jetzt auf die neuen Domains um möglicht viel PR (auch wenn der PR nicht wichtig ist) weiterzugeben?"

Den Originalthread kann man in diesem Forum nachlesen:

http://www.suchmaschinentricks.de/forum/thread.php3?thread=2939&forum=1

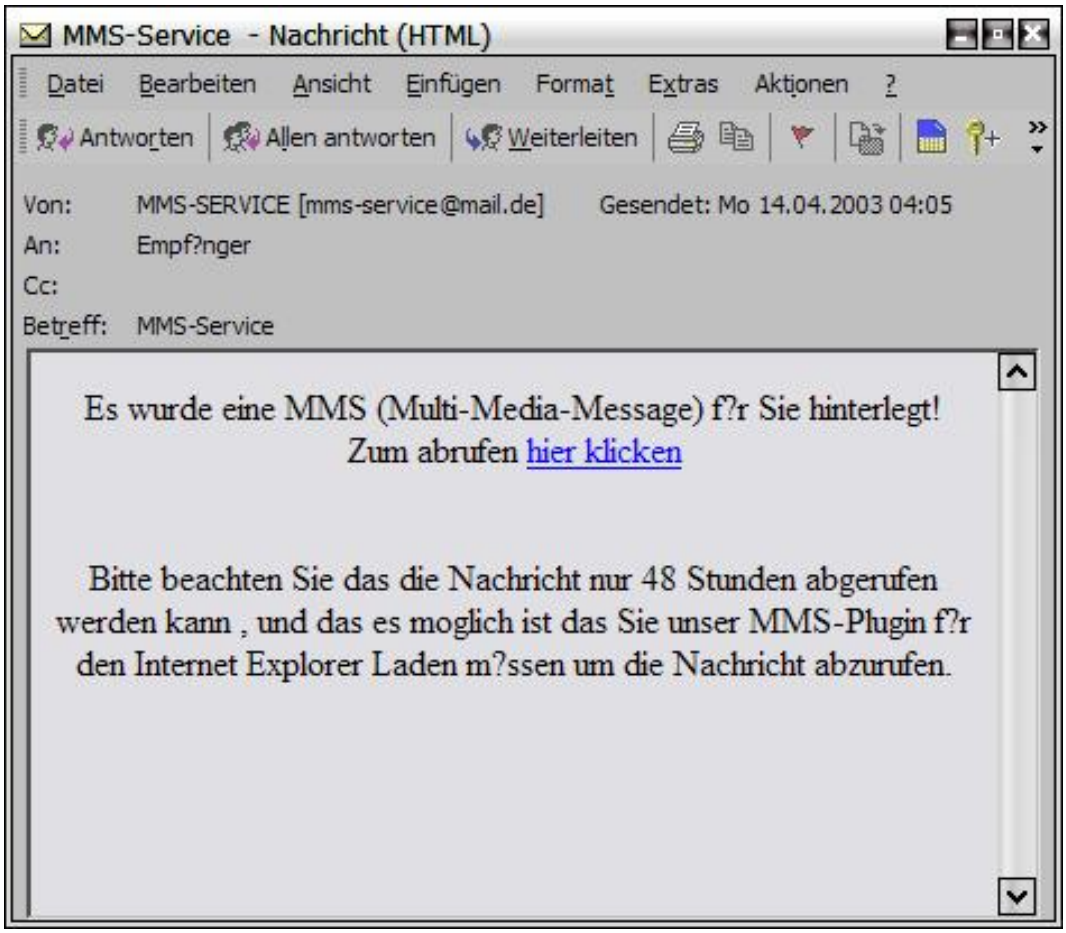
Eine weitere recht interessante und scheinbar geldbringende Masche ist die nachfolgende.
Mit steigendem Internetkonsum wachsen auch die Tricks der Hacker und Cracker im Internet, die auch zunehmend "normale" Internetuser interessieren.
Auf verschiedenen Seiten werden entsprechende "Hackertoolz" angeboten, die dann per direkter Einwahl zum Download bereit stehen.
Hierbei versteckt sich ebenfalls ein 0190-Dialer, der sich dann teuer über Ihren Computer einwählt!

Abzocke wird aber auch mit dem Geschäft der Lust betrieben.
Oftmals schreiben sich viele Menschen mit anderen und verwenden die Original E-Mail um direkt von dort zu antworten.
Auch hier wurde eine Masche entwickelt, die genau darauf abzielt.
Mit E-Mails die im Betreff "Re:" stehen haben versucht man vorzutäuschen, dass es eine Antwortmail sein sollte.
Hierbei handelt es sich fast immer um eine Werbemail von diversen Erotikseiten im Internet, die so Kunden ködern wollen.

Die neueste Methode der Abzocke sind E-Mails, die angeblich eine MMS enthalten oder wichtige Kundendaten für Sie bereithalten.
Direkte Zuweisungen von CLSIDs kann die Dateiendung geschickt versteckt werden und der vermeintliche Kunde wird mit einem Dialer aus dem Internet überrascht.

Sehr geschickt erscheint die Masche, dass man Kunden die kein MMS fähiges Handy besitzen die Möglichkeit

anbietet, diese an Sie gesandte MMS per Internet abzuholen. Von den Netzprovidern in Deutschland ist das durchaus eine übliche Form, jedoch verbergen sich hier betrügerische Gedanken dahinter und keine echte MMS. Vorsicht ist also geboten, wenn man also per E-Mail aufgefordert wird, eine MMS im Internet abzurufen.
Bei den Netzanbietern in Deutschland wird der Absender in der Regel mit übermittelt.



MMS Plugin ? Sicher nicht !

Eine weitere sehr gefährliche Masche ist die, dass für einen Kunden eine E-Mail mit der Kündigung verschickt wird und ein Guthaben angepriesen wird. Dies kann im einzelnen wie folgt aussehen:

Sehr geehrter Kunde,..... mit bedauern haben wir Ihre K?ndigung zur Kenntnis genommen.
Wie gew?nscht haben wir Ihren Zugang ab dem 01.05.2003 gesperrt.
Ihr Guthaben in Hohe von ? 274,80 werden wir auszahlen.

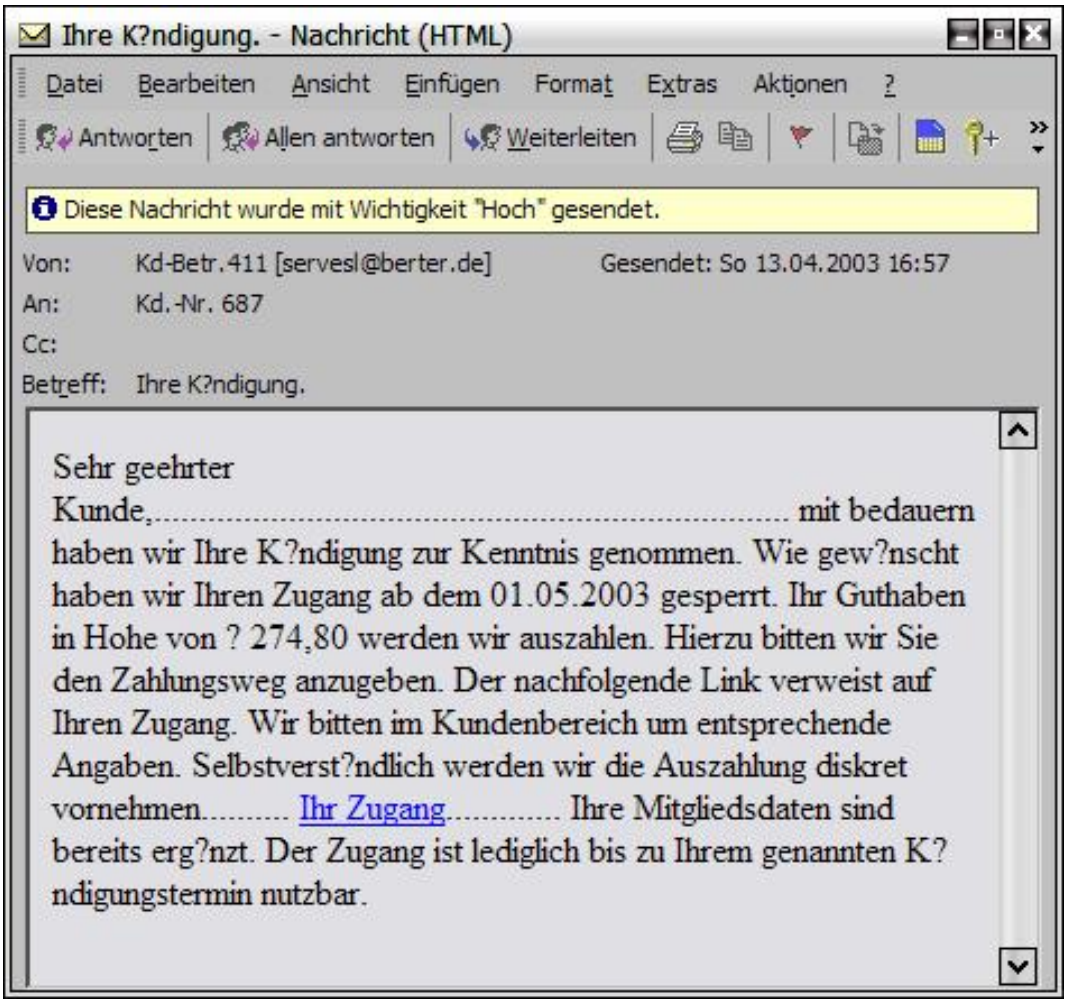
Hierzu bitten wir Sie den Zahlungsweg anzugeben. Der nachfolgende Link verweist auf Ihren Zugang.
Wir bitten im Kundenbereich um entsprechende Angaben.

Selbstverst?ndlich werden wir die Auszahlung diskret vornehmen..... Ihr Zugang..... Ihre Mitgliedsdaten sind bereits erg?nzt.
Der Zugang ist lediglich bis zu Ihrem genannten K?ndigungstermin nutzbar.

Sehr auffällig ist hier, dass diese E-Mail automatisch generiert wurde. Entnehmen kann man es der unpersönlichen Ansprache und den Fehlern bei "? 274,80" ohne Währungsangabe.

Der Zugang auf den man dann klicken soll sieht dann so aus:
http://xxxxxxx.supereva.it/portal.txt?sid=1C1413101C4222000401560F01084B5C0B5B5451034744510C405E440C045045565D02585B53.

Das es sich hierbei nicht um eine tatsächliche Kundenbetreuung handelt sollte auffallen.



Durch das versenden und laden einer SID ist es möglich, den Internetexplorer zu täuschen und einen Dialer auf den Computer zu laden auch wenn man gefährliche Skripte untersagt hat.
Ebenfalls werden sehr viele solcher E-Mails versendet, um eine angebliche E-Postkarte abzuholen, die dann aber über einen Dialer geladen werden soll:

Sehr geehrtes Mitglied,
fuer Sie wurde von(angelika_478ccg@web.de)
bei uns eine digitale Grusskarte hinterlegt.

Die Grusskarte kann innerhalb der naechsten 30 Tage unter
HYPERLINK "http://jarita1.tripod.com.ar/xxxxxx.txt?sid=021D0018085D2207131145131
A07175D194F03040841455A084B595F4102555F1941035B594C4A015F47"Grusskarte
von mir :-)abgerufen werden !
Wir wümschen Ihnen viel Spass !

Das komische daran ist jedoch, dass der Absender wieder ein anderer ist: angelika
[anhflika_xcd478cch621@web.de]

Wichtige Hinweise zur Ihrer eigenen Sicherheit:

* Öffnen Sie keine E-Mails deren Absender Sie nicht kennen!
* Klicken Sie nicht auf Links und Verweise ins Internet, deren Herkunft Ihnen nicht bekannt sind!
* Leiten Sie keine E-Mails mit Hinweisen weiter, dass man diese Mail weiterleiten sollte!
* Laden Sie sich ein Programm runter, dass die Verbindungen von 0190-Dialern untersagt sowie die neuen Nummern 0193, 0900 etc.!

Hier empfehle ich:
0190-Warner
http://www.wt-rate.de/

Wer mit Outlook oder Outlook Express arbeitet, der kann ein kleines "Tool" im Internet kostenlos erhalten, dass dann alle HTML E-Mails automatisch im Klartext darstellt und man so sehen kann woher eine Mail kommt.
NoHTML lesen und downloaden.

Weiterführende Informationen und Artikel zum Thema:

0190er Dialer, die Gefahr der Abzocke und Ausnutzung der User
Test zu den Programmen YAW und 0190-Warner sowie Teil 2
Hacking Intern :: Kapitel 7 ~ 0190 Dialer von seriös bis illegal

CLSID - Was ist das?
Mittels der CLSIDs können im Windows Systemfunktionen aufgerufen werden.
CLSID werden im Windows Betriebssystem beispielsweise dafür verwendet, um einzelne Dienste und Systemelemente in der Systemsteuerung direkt zu öffnen und nicht in einem extra Fenster zu öffnen.
CLSID benötigen keine Dateiendung um direkt ausgeführt zu werden und sind daher natürlich unter Verwendung eines direkten Links ein Sicherheitsrisiko.

Danke an Udo L. für die Korrektur und veränderte Vorschläge.
Aus meiner persönlichen Sicht kann ich anfügen, dass bisher die wenigen Menschen die 0190/0900-Dialer nicht als realistische Bedrohung erkennen und oftmals erst dann handeln wenn der erste Schaden eintritt.